Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1.   (Currently Amended) An information processing device comprising:

a data input interface for inputting encrypted data;

a decryption module for decrypting encrypted data inputted by the data input interface using a decryption key forming a pair with a first encryption key used to encrypt the data;

a deciding device for deciding whether or not to encrypt ~~data inputted by the data input interface, wherein the encryption module encrypts data decided upon for encryption by the deciding device;~~data decrypted by the decryption module;

an encryption module for encrypting data ~~decrypted by the decryption module~~ using a second encryption key different from the first encryption key; and

a storage device for storing data encrypted by the encryption ~~module.~~module, wherein the encryption module encrypts data decided upon for encryption by the deciding device.

2.   (Previously Presented) The information processing device of claim 1, wherein an expiration date is not set for the second encryption key.

3.   (Previously Presented) The information processing device of claim 1, wherein the data input interface also inputs unencrypted data, and the encryption module also encrypts unencrypted data input by the data input interface.

4.   (Previously Presented) The information processing device of claim 1, further comprising:

a key generator for generating the second encryption key.

5.   (Previously Presented) The information processing device of claim 4, further comprising:

    volatile memory; and

    a memory controller for storing the second encryption key in the volatile memory.

6.   (Previously Presented) The information processing device of claim 4, wherein the key generator generates the second encryption key using information characteristic to the device itself.

7.   (Previously Presented) The information processing device of claim 4, wherein the key generator generates the second encryption key when power to the device is turned on.

8.   (Previously Presented) The information processing device of claim 4, further comprising:

    a media reader capable of being installed with a removable portable storage media storing key generation parameters for reading a key generation parameter stored on the installed portable storage media, wherein the key generator generates the second encryption key using the key generation parameter.

9.   (Previously Presented) The information processing device of claim 4, further comprising:

    a device for setting a security level for the information processing device; and

    a device for storing the security level of the information processing device, wherein the key generator generates the second encryption key of a key length corresponding to the security level.

10.   (Previously Presented) The information processing device of claim 4, further comprising:

    a device for receiving settings for a region where the device is to be used; and

a device for storing the settings for the region of the information processing device, wherein the key generator generates the second encryption key of a key length corresponding to the region.

11. (Previously Presented) The information processing device of claim 1, further comprising:

a media reader capable of being installed with a removable portable storage media storing the encryption key, wherein the encryption module reads the second encryption key from the portable storage media installed in the media reader and performs encryption.

12. (Previously Presented) The information processing device of claim 1, equipped with a plurality of the storage devices, and having second encryption keys corresponding to each storage device, wherein the encryption module performs encryption using the second encryption key corresponding to storage device decided by a data storage destination.

13. (Previously Presented) The information processing device of claim 1, having encryption keys corresponding to each user using the device, wherein the encryption module performs encryption using an encryption key for the user corresponding to the data.

14. (Canceled)

15. (Previously Presented) The information processing device of claim 1, wherein the deciding device decides to encrypt encrypted data inputted by the data input interface and decrypted by the decryption module.

16. (Previously Presented) The information processing device of claim 1, further comprising:

a printer for decrypting and printing data stored in the storage device.

17. (Currently Amended) A method for storing data inputted to an information processing device, comprising the steps of:

inputting encrypted data;

decrypting encrypted data inputted using a decryption key forming a pair with a first encryption key used to encrypt the data;

deciding whether or not to encrypt ~~data inputted by the data input interface;~~ <u>data decrypted by the decryption module;</u>

encrypting decrypted data using a second encryption key different from the first encryption key; and

storing data encrypted using the second encryption key.

18.   (Previously Presented) The information processing device of claim 17, further comprising a step of:

storing the second encryption key in the volatile memory.